下载APP

14 | 安全：物联网平台如何应对安全风险？

2020-12-11 郭朝斌

物联网开发实战 进入课程 >

讲述：郭朝斌
时长 19:59 大小 18.31M

你好，我是郭朝斌。

在第 13 讲的思考题中，我提到了用户对于摄像头泄露隐私的担忧。这样的顾虑并不是杞人忧天。在现实生活中，物联网设备确实面临很多安全问题，而且这些安全问题已经对个人信息安全构成威胁。

比如 2019 年 12 月，在美国非常流行的家庭安防产品 Ring 爆出安全漏洞。黑客不但可以远程查看 Ring 的监控视频，还获取到了家庭 Wi-Fi 的密码，甚至可以把收集的用户音频数据分享到开放的播客节目中。

作为物联网开发人员或者安全技术负责人，我们肯定不想看到自己负责的产品和服务上负面新闻。为了跟用户建立信任，我们必须切实做好安全工作，打造可靠的产品和服务，保

护数据不被泄露。

你可能已经对于互联网的安全工作有一些了解，甚至有一定实践经验。不过在物联网领域有很多新的变化，所以我们需要重新思考安全工作该怎么开展。

在物联网设备上，安全的实践并不像在电脑上那么成熟。虽然现在的公司也越来越重视设备的安全问题，但是还是经常出现失误。

更何况，很多设备都是创业公司或者外包团队研发生产的。它们本身的盈利能力还比较弱，没有足够多的资源投入到安全方面，所以这些设备面临的安全问题往往更加严重。

总的来说，安全问题主要反映在两个方面：第一，公司没有针对物联网的特点建立起完善的安全管理流程和制度；第二，在具体的技术实践中，没有考虑物联网面临的新的安全问题。

所以在这一讲中，我就从管理和技术两个方面出发，跟你分享一些物联网的安全实践经验。

安全管理规范

首先，你需要建立一个**安全管理规范**，从机制和组织上保障安全，不能因为各方面资源的限制而放松要求。

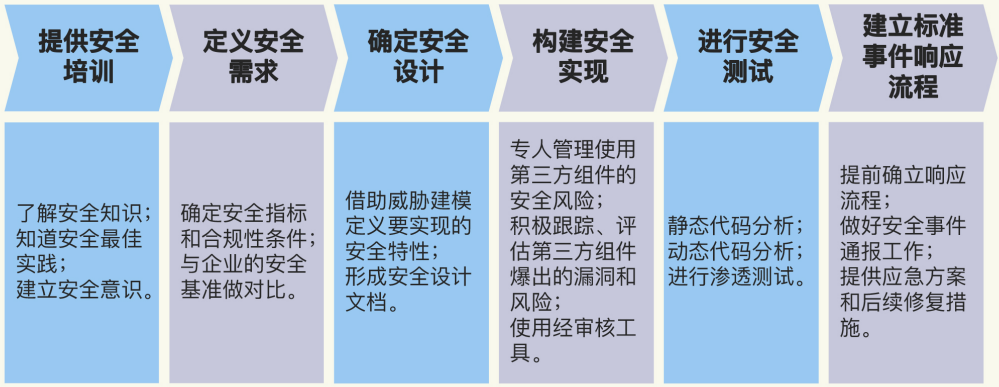
从实践的角度出发，我把安全管理分为**开发**、**生产**、**部署**和**运营**4 个方面。

1. 开发：基于安全开发生命周期建立流程

开发是产品和服务的基础，是最关键的地方，所以我先说说开发。

在开发过程中，怎么保证安全，满足合规性的要求呢？你可以基于**安全开发生命周期**（SDL，Security Development Lifecycle）来建立企业的安全开发流程。SDL 早已是保证开发安全的公认方法论。它能够减少安全漏洞的数量、降低安全漏洞的危害，从而帮助你做出更安全的产品和服务。

SDL 的整个周期由六个过程组成，我总结在了下面这张图片里。



2. 生产：降低由工厂带来的安全风险

跟纯软件产品不同，物联网设备还需要在工厂生产。那么，在生产中你要注意什么安全问题呢？注意，这里的“安全”不是指**人身安全（Safety）**，而是指**出厂设备的安全（Security）**。

首先，你在选择合作工厂的时候，要确保对方具备一定的**质量体系流程**，最好有第三方的质量体系认证。这样可以一定程度上保证工厂在流程上的安全工作。

其次，你在设计产品的时候，一定尽量**减少在工厂进行涉及安全的操作**，比如设置安全秘钥等。这样可以最大限度地减少工厂操作失误和数据泄露带来的问题。

最后，还有一些有安全风险的操作是必须在工厂进行的，比如设备固件烧录和硬件电路板组装等。对于这些操作，你要和工厂一起确定好流程，做好固件版本和硬件批次的控制，同时在**成品质量检测**中增加软、硬件版本的检查项目。

3. 部署：从软件和硬件两方面考虑

在物联网产品和服务投入正式使用之前，我们还需要进行软件和硬件的部署工作。为了保证系统的安全，你需要采取哪些措施呢？

一方面，你要做好**软件**的安全部署。

在服务器上部署软件的时候，你要检查防火墙的配置，保证不必要的端口都是关闭的。另外，软件的各种安全设置都要打开，不能让安全设计沦为摆设。

另一方面，你也要做好现场的**硬件**安全部署。

在现场部署硬件设备的时候，你需要考虑设备被随意获取、暴力拆解和分析的情况。因为拿到设备进行研究，往往是对物联网设备进行安全攻击的第一步。尤其是那些不能从商场买到的，或者部署在室外的非普通消费品，比如智能电表，还有无人值守停车场部署的计费设备等。

所以你得采取一定的**物理防护措施**，比如安装监控摄像头或者额外的防护装置（比如外壳等），让攻击者不能轻易地获取到设备。

另外，在设备初次入网或者重新入网的时候，你要保证**操作人员的可信度**，并做好**安全引导工作**。同时，你必须要求操作人员把设备的一些控制接口关闭，或者修改初始默认密码。比如对于网关设备，你可以关闭本地管理界面功能，或者修改初始的密码，这样可以避免被攻击者轻易地破坏。

4. 运营：把安全融入持续的运营过程中

最后，在产品和服务运营的过程中，我们还需要做好监控、运维和应急响应组织建设这 3 个方面的安全事项。

监控可以保证及时发现问题，是非常重要的运营手段。

比如，你可以通过系统实现**对设备和平台系统的日志进行自动化监控和分析**。这可以帮助你从一些记录中（比如系统尝试提权和认证异常等）及时发现异常行为。

还有一些监控发现的事件，是需要及时通知用户的。比如异常登录，系统要及时通过短信或者邮件告知用户风险。

运维是确保服务和设备安全状态的重要工作。

除了做好云平台服务器的运维工作之外，你还可以在系统中**增加设备资产的管理功能**，这有利于跟踪设备状态和固件更新等工作。

另外，很多物联网设备中存储有秘钥、证书等敏感信息。所以对于所有被淘汰的物联网设备，你都要做好**退役期处理**，把关键信息从设备上擦除掉，同时在云平台上对设备做归档、标记等处理。

应急响应中心是互联网公司在长期的安全实践中做出的非常好的创新。

在互联网发展的初期，一些“白帽子”黑客就算发现问题，也很难流畅地反馈给企业处理，甚至会被认为是勒索。但目前主流的公司基本上都会设置安全应急响应中心，甚至鼓励在一定的范围内**跟白帽子合作**，来提高系统的安全性。这是你在实践中值得借鉴的方法。

安全技术保障

刚才说的安全管理规范，只是从制度上来减少安全漏洞和安全事故，并对安全事件进行及时响应和处理。但是实际工作中，你还需要从技术上来保障安全。

怎么做好技术保障呢？我们知道物联网从架构上可以分为三层，设备层、网络层和应用层，你可以从这三个层面入手来做好安全工作。

现在我以共享单车为例做一个讲解。

第一步：分析安全需求

共享单车，你我都很熟悉，我们很容易就能分析出它的安全需求：

1. 保证单车资产的安全
2. 确保开锁、计费等关键功能和数据的完整性
3. 保证个人信息、轨迹信息等敏感信息的保密性
4. 确保云平台、App 等整体系统的可用性

接着，我们细化这些需求，列出明确的指标，然后跟公司的安全基线对比，看是否符合安全基线的要求，对于不符合的部分是否可以放行。

公司的安全基线是从哪里来的呢？一是公司自己的实践经验，二是最佳安全实践指导文件。

这些指导文件来自安全公司或者安全组织，比如国内的绿盟，国外的 CSA（Cloud Security Alliance，云安全联盟）、IIC（Industrial Internet Consortium，工业互联网联

盟）和 IoTSF（IoT Security Foundation，物联网安全基金会）等。

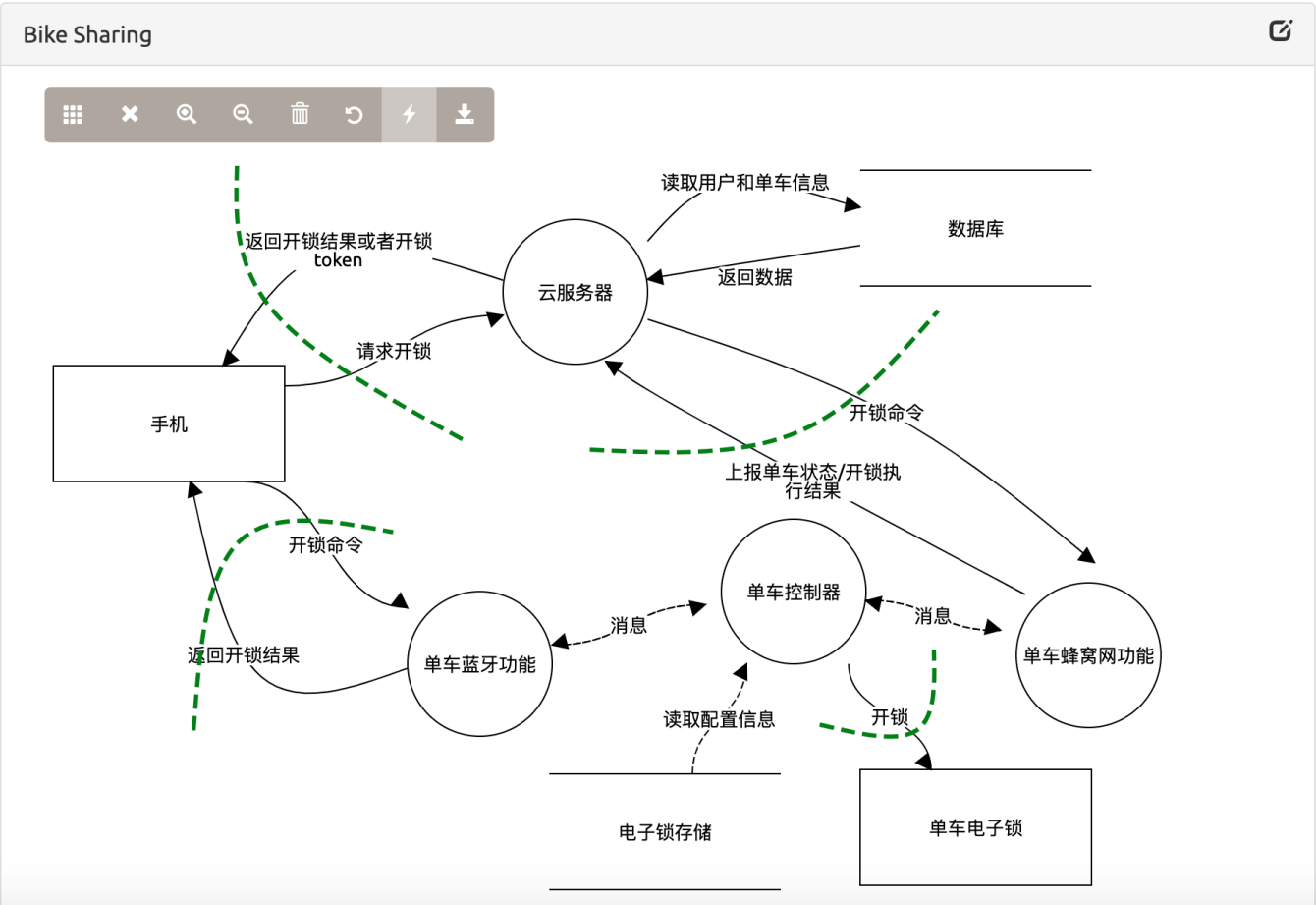
另外，还有一些行业相关规范涉及的安全内容，包括我在第 13 讲介绍的隐私相关法律法规对于安全防护的要求，这也是公司安全基线的一个来源。

第二步：构建威胁模型

明确了安全需求之后，下一步就是构建共享单车系统的威胁模型。建模可以帮助我们全面地了解共享单车系统中各个角色、接口和数据流，然后分析清楚系统面临的攻击面和信任边界。基于攻击面和信任边界，我们就可以更好地识别系统的潜在威胁。

至于建模的具体方法，我们可以使用 OWASP 提出的威胁建模备忘清单。它的好处是有一个开源的工具可以使用，名称是 Threat Dragon。除了这个，我们还可以选择微软的威胁建模工具，它也是免费的。

首先，我们基于共享单车系统的组成绘制出数据流图。下图是我使用 Threat Dragon 工具创建的共享单车系统的数据流图。（注意，这里只是举例，现实中的单车系统可能与此不同。）



共享单车数据流图

基于数据流图，我们就可以做威胁识别了。你可以借助微软的STRIDE 模型来完成，这也是 Threat Dragon 支持的威胁定义方法。

STRIDE 模型将威胁分为六种不同的类型：欺骗、篡改、否认、信息泄露、拒绝服务和权限提升，它们在下面的威胁识别表格中都有体现。

序号	威胁	类型
1	通过手机App获取用户账号或账号凭证，实现使用此用户账号使用单车	欺骗
2	通过破解蓝牙交互协议，伪造开锁指令使用单车	篡改
3	通过谎报单车电子锁故障，无法正常锁车，实现少计费或者免费使用等目的	否认
4	通过提取、分析单车电子锁的固件，获取秘钥等信息	信息泄露
5	通过实时DDoS攻击，使共享单车云平台无法提供服务	拒绝服务
6	通过在云平台服务器植入rootkit恶意软件，实现控制云平台系统的目的	权限提升
7	通过破坏车体二维码，使单车无法被其他人正常使用	拒绝服务
8	通过伪造单车电子锁发送锁车完成状态，实现少计费或者免费使用，甚至盗车等目的	篡改
9	通过SQL注入获取数据库的读写权限，获取到用户个人信息	信息泄露

共享单车威胁识别表

识别完威胁以后，我们需要归档，然后根据发生概率和可能的危害程度，对它们进行评估。评估可以使用微软的DREAD 模型来完成。它按照 5 个维度对一个威胁进行风险等级打分（分值范围 1～10），然后计算出平均值作为威胁的最后分数，分数越大风险越高。

对破坏车体二维码的威胁进行 DREAD 风险评分，可以得到表格所示的结果。

项目	细节分析	风险评分
潜在危害	单车无法被正常开锁使用	7
可重现性	被损坏的二维码无法自动修复，只能进行维修	8
可利用性	普通攻击者就可以实施这种破坏	8
受影响用户	接触到被破坏车辆的用户会受到影响	4
发现难度	攻击没有技术含量，很容易被发现并实施	9
平均分数		7.2

破坏车体二维码的威胁风险评分表

基于威胁评估的结果，我们可以对威胁的安全控制措施进行优先级排序，形成安全设计文档。然后我们把安全设计文档中的控制措施加入到产品的需求列表中进行跟踪，有计划地实施。

下面是我得到的共享单车系统的威胁矩阵，我按照物联网的三层架构进行了分组。

所属层级	威胁	风险评分
设备层	通过谎报单车电子锁故障，无法正常锁车，实现少计费或者免费使用等目的	7.6
	通过提取、分析单车电子锁的固件，获取秘钥等信息	6.6
	通过破坏车体二维码，使单车无法被其他人正常使用	7.2
网络层	通过手机App获取用户账号或账号凭证，实现使用此用户账号使用单车	5.2
	通过破解蓝牙交互协议，伪造开锁指令使用单车	5.6
	通过伪造单车电子锁发送锁车完成状态，实现少计费或者免费使用，甚至盗车等目的	6.2
应用层	通过实时DDoS攻击，使共享单车云平台无法提供服务	6.2
	通过在云平台服务器植入rootkit恶意软件，实现控制云平台系统的目的	5.4
	通过SQL注入获取数据库的读写权限，获取到用户个人信息	5.8

共享单车威胁矩阵表

接下来，我就分别讲解一下三层的安全控制措施。

第三步：逐层技术防护

设备层安全：业务目标的关键

首先是设备层。由于共享单车大多处于无人监控且恶劣的环境中，设备层的安全风险较为突出。

对于谎报电子锁故障，我们一方面可以在 App 中增加证据上报功能，比如图片、视频等，来增加谎报的难度；另一方面可以在电子锁上增加更准确和可靠的状态检测传感器，并且将这些信息上报服务器，这样就可以实现攻击识别的自动化，让攻击者不敢轻易尝试。

针对固件的攻击行为，实施成本较高，但对于专业人员来说也不是太大的难题，所以我们需要做好以下几个方面的防护措施：

1. 采取物理防护措施，加大拆除电子锁和拆解锁体的难度，让攻击者无法轻易获取到电子锁。
2. 采取篡改检测机制，通过传感器（比如压电薄膜）来检测破坏行为，然后声音报警，并且上报事件到云平台。
3. 在可能的情况下，尽量不启用芯片的调试接口（比如 JTAG 和串口），从而防止攻击者获取固件文件和控制接口。
4. 避免将敏感信息（比如加密私钥）硬编码到固件中，以防攻击者从硬件中获取到。

对于刚才提到的破坏二维码行为，最直接的方法当然是增加攻击难度，比如在车体多处增加二维码信息，采用更坚固的材料保护二维码。

不过，根本的办法还是寻找其他技术方案来替代二维码，或者作为二维码的备用方案，比如 NFC 和蓝牙技术。

网络层安全：加密通信是根本

然后是网络层。网络层面临的是不可控的传输网络，和未正确使用的通信技术，所以在物联网上传输的数据包如果没有加密和签名，很容易发生被窃听、篡改、伪造以及发送者抵赖等问题。

在 2017 年的GeekPwn 大会上，就有安全人员通过截获 Wi-Fi 网络上的数据包，轻松地获取了别人在 4 款共享单车 App 上的账号权限。他们靠这些权限，不但可以开锁，还能掌握用户的 GPS 轨迹等信息。这跟上面表格提到的，通过手机 App 获取账号和伪造电子锁发送关锁信息，属于类似的实现方式。

所以我们需要对网络通信进行加密，采用 **SSL/TLS** 的方法进行安全通信。在 App 上，可以采用 SSL Pinning 的模式进行双向认证，保证通信双方传输交换安全；电子锁设备的通

信也要加密，可以采用 MQTT 支持的 SSL/TLS 方式。

另外，蓝牙协议本身就支持很多安全机制，能够实现配对安全、数据防篡改和设备认证等特性。现在很多共享单车除了支持服务器下发命令开锁以外，还支持采用蓝牙协议来开锁。这时候一定要记得使用蓝牙的数据加密机制，保证开锁命令不会被攻击者轻易获取。

应用层安全：保证可用性和数据安全

最后是应用层。它作为物联网业务服务平台，向用户提供相关业务及应用。同时，在这个过程中，它还会采集、存储和处理大量的敏感数据。所以，我们必须保证服务的可用性和安全性。

DDoS 攻击可以说是目前最难防御的攻击之一，还没有特别完美的解决方案。我们可以采取多种方案组合，结合攻击的实际情况灵活应对，达到减少损失的目的即可。常用的手段有增加带宽，通过防火墙清洗，过滤异常流量，以及与专业的提供抗 DDoS 服务的公司合作。

对于上面威胁矩阵中提到的防范恶意植入和 SQL 注入，我们需要做好下面几件事：

1. 及时更新服务器操作系统和其他软件，尤其是出现严重漏洞的软件，不给攻击者可乘之机。
2. 设置防火墙，同时关闭不需要的服务和网络端口。暴露越少，被攻击的可能性就越小。
3. 定时对服务器和数据库做好备份，避免重要数据丢失或者服务不能及时恢复的情况。
4. 做好系统安全监控，及时发现异常的攻击行为，为进一步的安全防护做好准备。

另外，服务器对外提供的开放接口也可能导致的 SQL 注入等安全问题，同样需要注意。对于这些问题，我们可以通过定期做渗透测试来防范。

小结

总结一下，在这一讲中，我从安全管理规范和安全技术保障两个角度，讲解了我们在安全上需要关注的地方。

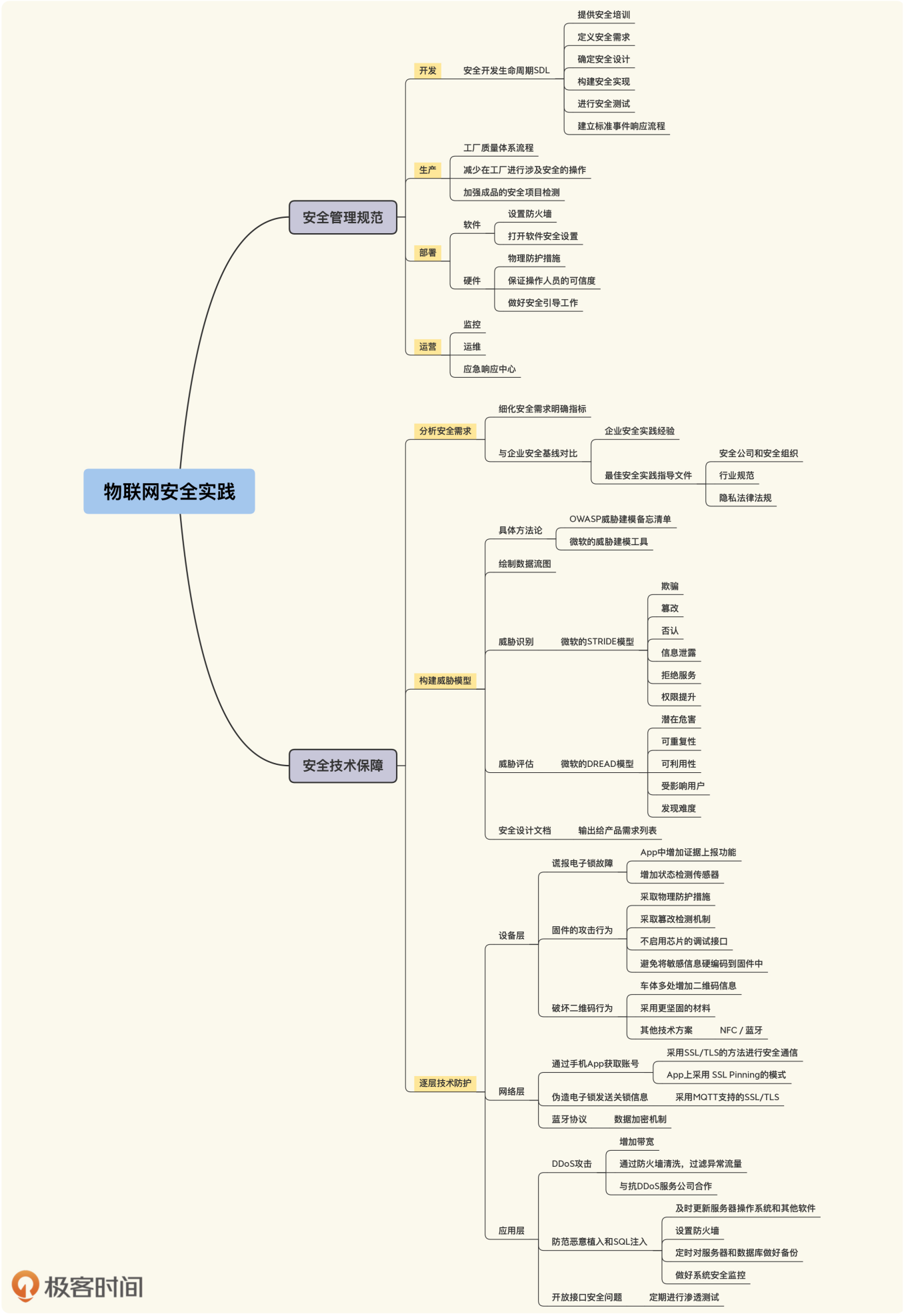
首先，我们要建立安全管理规范，从机制和组织上保障产品和服务的安全，主要分为四个方面：

1. 开发方面，我们可以基于 SDL 来建立企业的安全开发流程，保证开发符合安全规范。
2. 生产方面，通过质量体系、安全检查等保证出厂产品的合规。
3. 部署方面，既要注意软件的安全配置，也要保证硬件现场部署的安全措施落地。
4. 运营方面，我们需要做好监控、运维、应急响应组织建设这三个方面的安全事项。

其次，实际工作中，我们还需要从技术上来保障安全。具体步骤是先分析安全需求，再构建威胁模型，然后基于威胁建模的输出，在物联网三层架构中分别做好技术防护措施：

1. 在设备层中，做好固件、硬件接口上的防护工作。
2. 在网络层中，重点关注通信技术、通信协议的风险，保证网络通信采用 SSL/TLS 加密方式。
3. 在应用层中，做好 DDoS 攻击、SQL 注入等安全防护，及时处理安全漏洞。

我整理了一张思维导图，供你参考。


物联网安全实践
安全管理规范
开发
安全开发生命周期SDL
提供安全培训
定义安全需求
确定安全设计
构建安全实现
进行安全测试
建立标准事件响应流程
生产
工厂质量体系流程
减少在工厂进行涉及安全的操作
加强成品的安全项目检测
部署
软件
设置防火墙
打开软件安全设置
硬件
物理防护措施
保证操作人员的可信度
做好安全引导工作
运营
监控
运维
应急响应中心
安全技术保障
分析安全需求
细化安全需求明确指标
与企业安全基线对比
企业安全实践经验
最佳安全实践指导文件
安全公司和安全组织
行业规范
隐私法律法规
构建威胁模型
具体方法论
OWASP威胁建模备忘清单
微软的威胁建模工具
绘制数据流图
威胁识别
微软的STRIDE模型
欺骗
篡改
否认
信息泄露
拒绝服务
权限提升
威胁评估
微软的DREAD模型
潜在危害
可重复性
可利用性
受影响用户
发现难度
安全设计文档
输出给产品需求列表
逐层技术防护
设备层
谎报电子锁故障
App中增加证据上报功能
增加状态检测传感器
固件的攻击行为
采取物理防护措施
采取篡改检测机制
不启用芯片的调试接口
避免将敏感信息硬编码到固件中
破坏二维码行为
车体多处增加二维码信息
采用更坚固的材料
其他技术方案
NFC / 蓝牙
网络层
通过手机App获取账号
采用SSL/TLS的方法进行安全通信
App上采用 SSL Pinning的模式
伪造电子锁发送关锁信息
采用MQTT支持的SSL/TLS
蓝牙协议
数据加密机制
应用层
DDoS攻击
增加带宽
通过防火墙清洗，过滤异常流量
与抗DDoS服务公司合作
防范恶意植入和SQL注入
及时更新服务器操作系统和其他软件
设置防火墙
定时对服务器和数据库做好备份
做好系统安全监控
开放接口安全问题
定期进行渗透测试

从用户的角度看，安全和隐私可以说是密切相关。用户担心产品的安全问题，主要关注点也是害怕个人信息的被泄漏和滥用。作为从业人员，我们只有做好安全工作，才能落实好个人信息的保护，从而打造出安全可靠、用户信任的产品和服务。

思考题

最后，我给你留一个思考题吧。

我在第 7 讲介绍零配置组网时提到了 UPnP 协议。它为我们日常使用设备提供了便利，但也被称为“安全重灾区”。你知道 UPnP 协议存在哪些安全风险吗？

欢迎在留言区写下你的答案和我交流，也欢迎你将这一讲分享给对物联网安全感兴趣的朋友，大家一起讨论学习。

提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 13 | 隐私：在实践中如何保护用户隐私？

下一篇 15 | 平台：智能家居开源平台的生态是怎样的？

精选留言 (4)

写留言

YueShi 置顶

2020-12-15

这是一篇讲物联网安全的文章
同时不仅仅讲的是IoT行业
目前阶段的各个行业都是同样的道理
在行业发展/企业发展上走大干快进的路子
走先污染再治理的老路子...

展开

1 1

qinsi
2020-12-11

所以有时候我们在路上看到两个监控摄像头面对面安装是为了各自防止对方被窃吗……

作者回复: 呃，观察够细致的👍
也可能为了不同角度

4

il李li
2020-12-14

关于网络层通信技术采用SSL/TLS加密通信方式，目前大部分TLE、WiFi终端硬件资源、网络协议栈能支持运行，不过还有些低端产品资源不足无法支撑，需要在硬件选型阶段做充分的考虑，对于平台接入侧维持海量设备的TLS接入也需要几部于TCP的计算资源。可以根据场景区分，比如：终端状态定时上报只需要做数据签名保障完整性；控制指令下发必须基于TLS安全通道

展开

1

莹
2020-12-20

能想到关于UPnP协议的几个风险：
- 如果即插即用设备有病毒或者恶意程序，那么插入后是不是可能会导致一些网络层的信息泄露
- 分配IP时是不是有可能收到攻击